**REMARKS**

The Examiner has objected to an informality on page 1 of the application. The relevant sentence has been rewritten to correct this informality.

The Examiner has rejected claims 4, 5, 7 and 10 on the basis of insufficient antecedent basis for the phrase "said one bit string" This phrase has been revised to read "one of said bit strings" as suggested by the Examiner. Accordingly, the rejection is believed to be overcome.

The Examiner has rejected claim 1 under 35 USC 103(a) as unpatentable over McCollom (EP 0 918 274) in view of Coron et al. (XP-002192618). The Examiner contends that although McCollom does not describe the message being split into two parts that Coron et al. describes splitting a message into two parts and then it would have been obvious to combine these teachings.

Applicant has carefully reviewed the references cited by the Examiner and offers the following comments.

Applicant respectfully believes that the word "fingerprint" and "signature" as used in McCollom do not refer to a digital signature of the type described in the present application. Referring to page 1 of the present application, it is noted that digital signatures are generated by signing a message with the originator's private key. In the system of McCollom, there is no private key used by the sender. The same keys are required on both ends of the communication so there is no provision for uniquely binding the fingerprint to the sender. This means that the scheme in McCollom does not provide non-repudiation of the fingerprint. In other words, the sender does not have the exclusive ability to provide the fingerprint.

Applicant notes that the cited portion of the Coron reference is actually referring to the ISO 9796-2 signature scheme. This scheme is in fact described in the application at the top of page 2. As noted in the application, this scheme does not achieve bandwidth efficiency and requires the computation of two hash functions.

Amended claim 1 recites that the second signature component is provided using the private key and therefore distinguishes over McCollom for the reasons above. In the system of amended claim 1, the signer uses its private key (which is maintained as a secret) and the signature scheme therefore provides non-repudiation.

The Examiner has suggested that it would be obvious to combine McCollom and Coron.

However, the Examiner has not shown any motivation for such a combination. In fact, the systems described in the two references are substantially different. The Examiner has not provided any indication of why these could be combined and why such a combination would produce a viable method. Furthermore, the Coron reference which was cited does not contain any discussion of how the ISO 9796-2 signature scheme operates. The Examiner has relied only upon a comment that a message is split into two parts. According the rejection under 35 USC 103(a) is believed to be overcome.

Claims 2 through 6 are dependent upon claim 1 and the rejections under 35 USC 103(a) also rely on McCollom and Coron. Accordingly, it is believed that these objections are overcome by the comments above.

Claim 7 has been rejected under 35 USC 103(a) as unpatentable over McCollom in view of Corol et al and Kitaori et al (US 5,915,024). As noted above, Applicant respectfully believes that McCollom does not teach a digital signature in the sense of the present patent application. Amended claim 7 recites that the signer has "a private key used in the computation of said signature and a corresponding public key available for use in verification". The Examiner has acknowledged that McCollom does not teach several features of claim 7. Accordingly claim 7 distinguishes over the disclosure in McCollom.

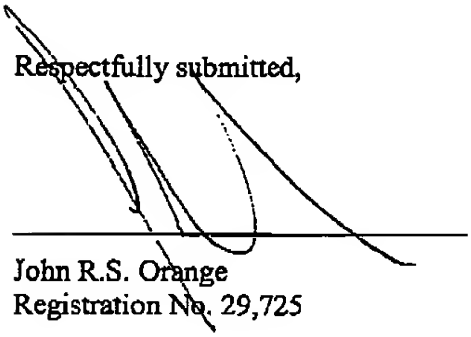
The Examiner has contended that it would be obvious to combine McCollom with Coron et al and Kitaori et al to obtain the subject matter of claim 7. For the reasons given above in respect of claim 1, Applicant believes that it would not be obvious to combine McCollom and Coron et al and the rejection is therefore believed to be overcome. Furthermore, the Examiner has relied upon Kitaori for disclosure of using information of the signer in the digital signature process. The cited portion of Kitaori describes including information about the signer in certain fields, but does not describe how this information is used and the manner in which calculation are made. Moreover, the Examiner has not shown any specific reason, motivation, or teaching to combine the cited references. Even if such a combination were possible, combining Kitaori with McCollom and Coron would therefore not give a digital signature process with a private key and public key pair with each key used appropriately in the signing and verifying processes.

Claim 8 through 10 are dependent upon claim 7. These claims have been rejected under 35 USC 103(a) and overcome the rejection by their dependence on claim 7 for the reasons above.

Furthermore, Applicant notes that the rejections to claims 2-5 and 8-10 each use at least four different references and refer to single sentences within the additional references as providing additional features. Applicant respectfully believes that the Examiner has not found motivation to combine these references and the in some cases the cited portions have been taken out of context. Applicant respectfully believes that a combination of four or more references in an obviousness rejection is prima facie improper. Accordingly, Applicant traverses the comments made by the Examiner in respect of these dependent claims 2-5 and 8-10 that it would be obvious to make various combinations of Coron with Menezes et al, Nyberg, ISO-IEC 9796-1 and Kitaori et al.

Applicant respectfully requests reconsideration of the Examiner's objections.

Respectfully submitted,



John R.S. Orange
Registration No. 29,725